5. Border Officials Do Not Receive the Intelligence They Need to Perform Their Counter-Terrorism Mission

Three years after 9/11, antiquated intelligence databases available to frontline border officials are not fully integrated or interoperable. Millions of travelers are still not checked against any database. Unintended intelligence stovepipes have formed within border agencies with a proliferation of uncoordinated and duplicative intelligence centers. Complicating this is the fact that the vast majority of border investigators lack clearances to work their number one priority – counterterrorism.

More and better intelligence is needed to secure our borders. In a July, 2004 congressional hearing, Customs and Border Protection Commissioner Robert C. Bonner acknowledged the need for better intelligence for border agents and inspectors. He stated the "majority of CBP seizures were the result of "cold" hits…not the result of actionable intelligence or information received from other agencies." He added "the need for border awareness, i.e. actionable and strategic intelligence has never been greater…the means to bring together all threat information is needed in order to significantly increase effectiveness to terrorists and terrorists weapons."[145]

Commissioner Bonner's candid admission was confirmed by the work of the 9/11 Commission, which placed great emphasis on interoperability and the sharing of information between government agencies. It noted that the greatest impediment to "connecting the dots" was the "systemic resistance to sharing information."[146]

Indeed, the Commission documented the many failed opportunities to identify and stop the 9/11 terrorists by U.S. immigration, customs and law enforcement personnel. They noted that in the months leading up to September 11, the government officials adjudicating the entries of the hijackers did not have adequate information on them even though such information was already in various databases maintained by a number of government agencies.[147] If the patchwork of intelligence databases had been properly merged the inspectors adjudicating entries may have detected the 9/11 hijackers. These problems still exist at our Southern Border.

Millions Entering the United States Are Still Not Checked Against Any Databases

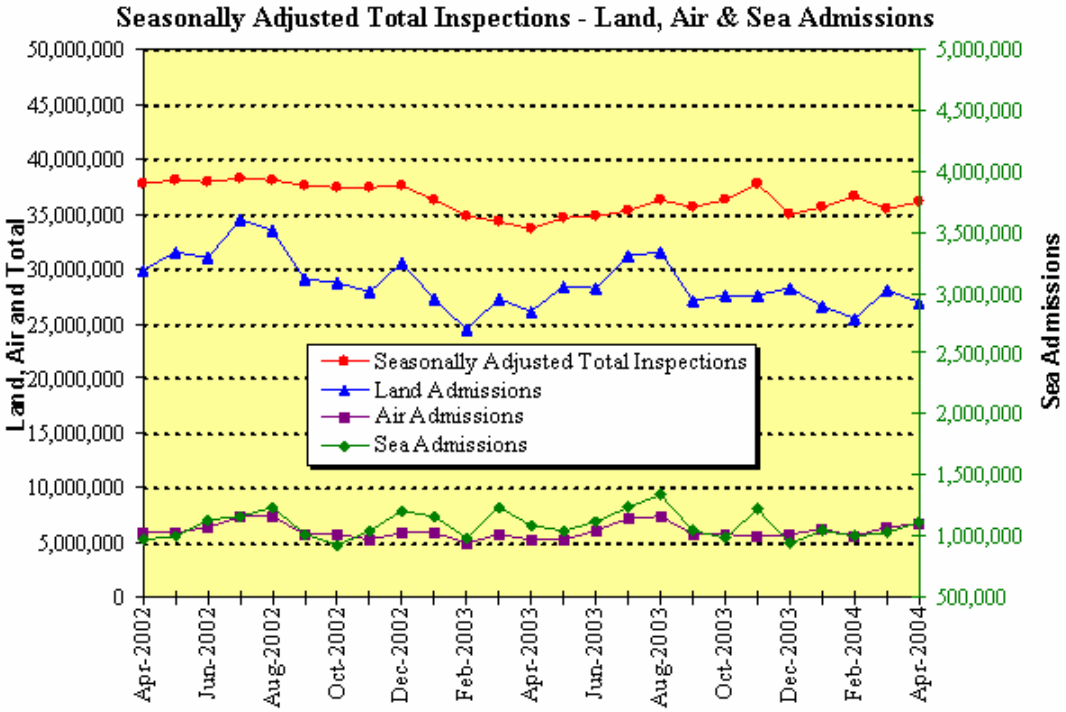
The 9/11 Commission called targeting the travel of terrorists one of the most important tools in our government's arsenal to stop terrorism. [148] However, most travelers entering the United States at our land borders are still not checked against any databases.[149] Millions enter without their names being checked against any terrorist watch list or other law enforcement database of known or suspected criminals. Currently, the primary means of defense for millions crossing our Southern Border is a cursory inspection by a border official that usually lasts less than a minute.

As indicated in the charts below, in fiscal year 2003 there were a total of 427,690,094 inspections of those seeking entry into the United States. Of this total, approximately 80% or 38,297,020 inspections were conducted at land ports-of-entry.[150] Of these an estimated 85% or approximately 287 million, arrive in vehicles.[151]

---

[145] *Op. cit.*, Bonner Testimony of July 22, 2004.
[146] 9/11 Commission Report, p. 416.
[147] *Ibid.,* p. 383-389.
[148] *Ibid.*, p. 385.
[149] Similar finding in: U.S. Government Accountability Office, *Land Border Ports of Entry: Vulnerabilities and Inefficiencies in the Inspection Process,* GAO-03-782*,* (Washington, D.C.: July 2003), p. 2; and Data Management Improvement Act (DMIA) Task Force, First Annual Report to Congress, December 2002.
[150] U.S. Citizenship and Immigration Services, "Inspections," found at: http://uscis.gov/graphics/shared/aboutus/statistics/msrapr04/INSP.HTM
[151] *Op. cit*., GAO-03-782, p. 8.

	Month			Fiscal Year			Total
	Apr-2004	Apr-2003	% Change	FY2004 to Date	FY2003 to Date	% Change	FY2003
Total Inspections	35,272,026	32,912,646	7	242,372,362	241,587,871	0	427,690,094
Air Admitted	6,727,122	5,263,674	28	41,995,628	38,859,610	8	70,690,316
Land Admitted	26,946,302	26,107,526	3	190,144,577	192,004,983	-1	338,297,020
Sea Admitted	1,124,469	1,083,077	4	7,358,904	7,666,939	-4	13,458,254
Inadmissible	55,430	52,595	5	353,428	381,707	-7	673,966



Source: U.S. Citizenship and Immigration Services

While the primary inspector at vehicle lanes has the discretion to check a traveler's name against the main lookout database, most travelers are not checked.[152] Rather, only the vehicle's license plate is checked automatically by a license plate reader located at each inspection lane. As the vehicle enters the primary inspection lane, the license plate reader checks the registration and name of the registered owner of the vehicle with a multi-agency lookout system called the Interagency Border Inspection System (IBIS).[153] It will advise the inspector if the vehicle is

[152] *Ibid*., p. 16.

[153] The Interagency Border Inspection System (IBIS) is a shared database of lookout and enforcement data contributed by two dozen Federal agencies, including the Department of State, legacy Immigration and Nationality Service, legacy U.S. Customs Service, Department of Agriculture, and the FBI. DHS lookout information is provided through the National Automated Immigration Lookout System (NAILS) into IBIS. The 14 year old IBIS system interfaces with the following systems: Department of State Consular Lookout and Support System (CLASS), Consolidated Consular Database (CCD), and the Claims 3, FBI (NCIC), and legacy INS systems to include Central Index System (CIS), Deportable Alien Control System (DACS), Refugee, Asylum, and Parole System (RAPS), Student Exchange Visitor Information System (SEVIS), Arrival Departure Information System (ADIS), Advanced Passenger Information System (APIS), Portable Automated Lookout System (PALS), TIPOFF, NVC, VWPASS, NSEERS, and the Non-Immigrant Information System (NIIS) which consolidates the multiagency "lookout" checks into one primary query.

legally registered, to whom it is registered, as well as the recent history of border crossings for that vehicle. It also will check the name of the "registered owner" against lookout and terrorist data bases – but only the registered owner, not the driver, if different, or any of the occupants of the vehicle unless they are manually entered into the system to be checked.

From interviews and observation of the inspection process, it is clear that inspectors may, but rarely do, run the driver or passenger(s) names through the IBIS system or any other database due to time pressures on the border. In the vast majority of cases, the inspector merely glances at the identification of the driver and passenger(s) and asks a few questions, usually to the driver, concerning his nationality and purpose for entering the country. As reported by GAO and confirmed by staff observations, this entire process takes less than a minute, with many inspections observed taking less than 20 seconds.[154]

Significantly, this is the full extent of the inspection process for 98%, or over 281 million, visitors annually entering our land borders by vehicle.[155] Consequently, this process leaves millions of travelers entering the country without being checked against any intelligence database that could help identify a potential terrorist or even a convicted criminal.

Compounding the intelligence shortfall, interviews with inspectors indicated that IBIS is an aging system that often breaks down. CBP agents report that it is inoperable ranging from less than 10% to as much as 33% of the time. Additionally, one inspector in California reported that IBIS is of little use because almost all smugglers use stolen vehicles therefore an IBIS query will give the primary inspector no intelligence information.[156]

US-VISIT was cited by some as a possible answer to the intelligence problems at the primary inspection stations. However, currently US-VISIT is only scheduled to be placed in the secondary examination area where only 2% of all land border examinations occur.

Interoperability of Databases Needed for Inspection Integrity – Inspectors Must Query as Many as Eight Databases with Eight Distinct Passwords

During the primary inspection process, if irregularities are noticed, the traveler or vehicle is referred to secondary examination. Approximately nine million, or 2%, of all travelers at land ports-of-entry were referred to more intensive secondary examination.[157] The intelligence databases used at secondary have not been merged and are not interoperable. Depending on inspections conducted, the inspector at secondary may have to log in and out of eight separate databases requiring eight unique password configurations that may expire as often as every 30 days.

[154] *Op. cit*., GAO-03-782, p. 7.
[155] *Ibid*, p. 16.
[156] The inspector stated that smugglers use stolen vehicles because the IBIS system at primary inspection will only report the registered owner of the vehicle and the number of times the vehicle has crossed the border. Additionally if apprehended, the violator will lose only the stolen vehicle, and not there own.
[157] *Op. cit.,* GAO-03-782*,* p. 9.

The secondary inspectors found this process to be burdensome and time consuming. They reported that the process of entering the same traveler information and remembering frequently changing passwords in each query was counter-productive and cumbersome. These procedures slowed the secondary inspection process, took inspectors away from other duties, and increased the chance that an inspector would forget to check a particular database resulting in a wrong decision about a traveler's admissibility.[158]

The 9/11 Commission criticized such stand alone systems and recommended that the Department of Homeland Security complete "as quickly as possible, a biometric entry-exit screening system" that combined all of these databases. The Commission noted that:

> The current patchwork of border screening systems, including several frequent traveler programs, should be consolidated in the US VISIT system to enable the development of an integrated system, which in turn can become part of the wider screening plan we suggest.
>
> All points in the border system – from consular offices to immigration services offices – will need appropriate access to an individual's files. Scattered units at Homeland Security and the State Department perform screening and data mining; instead a government-wide team of border and transportation officials should be working together.
>
> A modern border and immigration system should combine a biometric entry-exit system with accessible files on visitors and immigrants, along with intelligence on indicators of terrorist travel.[159]

Congressional and Executive Branch Plans to Build an Interoperable Border Security System Still Not Met

The need for integration and interoperability is not new. After the terrorist attacks of September 11, 2001, Congress and the Administration reached a consensus on the need to eliminate various obstacles to information sharing. In passing the USA PATRIOT Act six weeks after the 9/11 attacks, Congress urged rapid development of an "integrated entry and exit data system" and required the development of a biometric technology standard as the "basis for a cross-agency, cross-platform electronic system that is a cost-effective, efficient, fully integrated means to share law enforcement and intelligence information" for entry-exit screening.[160]

In May, 2002, Congress expanded upon this theme in Section 202 of the Enhanced Border Security and Visa Entry Reform Act of 2002, in which it mandated the creation of an "interoperable law enforcement and intelligence data system… to provide current and immediate access to information in databases of Federal law enforcement agencies and the intelligence

[158] *Ibid.*, p. 28.
[159] 9/11 Commission Report, p. 388-389.
[160] *USA PATRIOT Act*, 2002, Public Law 107-56, Title III, Section 403 (c) (2).

community that is relevant to determine whether to issue a visa or to determine the admissibility or deportability of an alien (also known as the Chimera system)."[161] In July 2002, the Senate Commerce, Justice, State Appropriations Subcommittee appropriated $83 million for the Chimera system, noting that "it will serve as the searchable, shareable repository of data bases migrated from existing (legacy) INS systems that are incompatible with one another and with other law enforcement, State Department, and intelligence community systems."[162]

A strong consensus on the importance of creating an interoperable border security system had also developed in the Executive Branch. In January, 2003, the Bush Administration submitted a detailed plan to Congress that outlined the major investments that would need to be made in the INS, FBI, and State Department to build a fully interoperable system, including biometrics, which could meet the counterterrorism goals required after September 11. It further stated that unless a cross-agency, "end-to-end" concept of operations were developed "before major investments are made, the estimated cost and expected results of the investment will be at risk."[163]

Soon after the Department of Homeland Security was created, it appeared to be in accord with the White House plan as its budget justification for fiscal year 2004 (submitted in February 2003), noted the importance of these programs and stated that:

> Atlas/Chimera is the infrastructure platform that will enable the DHS to meet requirements stipulated in the Border Security Act….. DHS will not be positioned to enhance its data sharing efforts throughout DHS (let alone with other Federal, State and Local law enforcement entities) through our Entry-Exit System initiative without funding for Atlas/Chimera to provide critical information technology infrastructure pieces as the foundation for these efforts. (Emphasis added).

In March, 2003, Undersecretary Asa Hutchinson reiterated DHS' commitment to proceeding with Chimera. At a hearing of the Senate Judiciary Committee, Undersecretary Hutchinson was asked if $245 million appropriated for fiscal year 2003 would be "dedicated to the interoperable systems such as Chimera?" He responded, "The answer is yes. We're working very diligently to accomplish the goals of the interoperable system."

Unfortunately, this integration has not occurred on the Southern Border. As described to the staff by various border enforcement personnel, this continues to cause critical problems with the ability of border agencies to effectively identify potential terrorists.

---

[161] Public Law 107-173, Title II, Section 202 (a) (2).
[162] Senate Report 107-218, Fiscal Year 2003 Department of Commerce, Justice and State, the Judiciary, and Related Agencies Appropriations Bill.
[163] Report to Congress submitted jointly by the Attorney General, Secretary of State, and the National Institute of Standards and Technology, *Use of Technology Standards and Interoperable Databases with Machine-Readable, Tamper-Resistant Travel Documents,* January 2003, p. 24.

Key Databases Still Not Integrated

Failure to integrate various intelligence databases into an interoperable system that could be used by front-line agents has been a particular problem for the Border Patrol. On average, the Border Patrol apprehends more than one million illegal immigrants a year attempting to enter the United States. The Border Patrol must quickly determine the identity of those apprehended illegal immigrants in order to determine which are a danger to our country and thereby should be detained for prosecution.[164]

Two separate databases must be searched to correctly make such a determination. These are the legacy-INS IDENT system and the FBI's IAFIS system.[165] They are not integrated despite calls since 1998 by the Department of Justice Inspector General that they need to be.[166] Their integration has moved slowly and still may take years to complete.[167] Two cases arising from the Southern Border demonstrate the tragic consequences of the failure to adequately integrate these systems.

In 1998, Rafael Resendez-Ramirez (Resendez), a Mexican citizen with an extensive criminal record inside the United States, was apprehended by Border Patrol in Texas and New Mexico seven times while illegally crossing the border. Because Ramirez had been apprehended fewer times than the threshold for prosecution, he was returned to Mexico.[168] In 1999, state and federal warrants were issued for Resendez for connection to several murders. Border Patrol again apprehended Resendez for illegal entry and again returned him to Mexico. They did not the check the FBI's IAFIS system, which would have detected the outstanding warrants. Within days, Resendez illegally crossed the border and committed four murders.[169]

In January 2002, Victor Manual Batres (Batres), a Mexican citizen with an extensive criminal record to include kidnapping, narcotics violations, and robbery, was apprehended twice

---

[164] Aliens may be detained for prosecution based on multiple illegal entries, reentry after deportation, arrest warrant, terrorist links, or for aggravated felonies delineated in Title 8 U.S.C. sec. 1101 (a) (43).

[165] The IDENT system, which began in 1994, is the "Automated Biometrics Identification System." To place an individual in the IDENT system, the right and left index fingers are placed on the scanner, a photograph is then taken with the IDENT camera and biographical information is entered into the computer. IDENT then electronically compares the fingerprints to a legacy INS "lookout" database and "recidivist" database. The IAFIS system, which began in 1999, is the "Integrated Automated Fingerprint Identification System" run by the FBI. It contains more than 40 million ten-print fingerprint records in its criminal master file. Fingerprints submitted are electronically compared against IAFIS records for "hits."

[166] See, U.S. Department of Justice, Office of Inspector General, *Review of the Immigration and Naturalization Service's Automated Biometric Identification System,* (Washington, D.C.: March 1998); U.S. Department of Justice, Office of Inspector General, *The Rafael Resendez-Ramirez Case: A review of the INS' Actions and the Operation of its IDENT Automated Fingerprint Identification System*, (Washington, D.C.: March 2000); U.S. Department of Justice, Office of Inspector General, *Status of IDENT/IAFIS Integration*, (Washington, D.C.: December 2001); U.S. Department of Justice, Office of Inspector General, *Status of IDENT/IAFIS Integration*, (Washington, D.C.: June 2003); and U.S. Department of Justice, Office of Inspector General, *IDENT/IAFIS*: *The Batres Case and the Status of the Integration Project*, (Washington, D.C., March 2004).

[167] U.S. Department of Justice, Office of the Inspector General, *IDENT/IAFIS*: *The Batres Case and the Status of the Integration Process*, (Washington, D.C.: March 2004).

[168] The staff found, during interviews, that the threshold number of apprehensions before prosecution widely varies on the Southern Border from as few as six to as many as 15.

[169] On May 21, 2003, Resendez' capital murder conviction and death sentence were affirmed.

in two days as he illegally crossed the border into the United States. Both times, Batres was returned to Mexico after conducting an IDENT check which was not integrated with the FBI IAFIS database. If the IAFIS and IDENT databases had been interoperable, it would have shown aggravated felony convictions and prior deportations which generally carry substantial prison terms. Instead, Batres illegally reentered the United States, traveled to Oregon where he brutally raped two Catholic nuns, resulting in the death of one of the nuns.

The Department of Justice Inspector General noted that Resendez and Batres cases could have been avoided if they had been checked in a unified IDENT/IAFIS database. These cases "tragically illustrated the danger of requiring immigration agents at individual Border Patrol stations to decide when they should research an apprehended alien's criminal history rather than relying on an integrated database…"[170]

Despite this criticism, these systems are still not integrated and as the Department of Justice Inspector General noted in his March, 2004 report, these problems could happen again. The Inspector General report concluded that only 12% of all ports-of-entry and 20% of all Border Patrol sites have access to an integrated IDENT/IAFIS database. The staff observed only two Border Patrol stations, Laredo, Texas and Nogales, Arizona, with fully integrated IDENT/IAFIS databases. The Presidio, Texas, station lacked any IAFIS machines. The Nogales integration has resulted in the identification of 21 illegal aliens with criminal records per day, on average.

Progress continues to move slowly, partially as a result of attention placed on other technology projects such as US-VISIT, and interoperability is still years from completion.[171] On July 26, 2004, DHS personnel reported that full interoperability with IAFIS was still two to three years away.[172]

Detection of Fraudulent Documents a Major Concern

A serious homeland security concern on the Southern Border involves the use of fraudulent documents by terrorists to conceal their true identity or to otherwise obtain entry into the country by falsely claiming U.S. citizenship. The recent 9/11 Commission Report brought this issue into focus by noting the importance of false documents to terrorists:

> For terrorists, travel documents are as important as weapons. Terrorists must travel clandestinely to meet, train, plan case targets, and gain access to attack. To them, international travel presents great danger, because they must surface to pass through regulated channels, present themselves to border security officials, or attempt to circumvent

[170] U.S. Department of Justice, Office of Inspector General, *IDENT/IAFIS: The Batres Case and the Status of the Integration Project,* (Washington, D.C.: March 2004), p. 15.
[171] *Ibid.,* p. 39.
[172] Staff meeting with U.S. Department of Homeland Security, US-VISIT staff on July 26, 2004.

> inspection points. In their travels, terrorists use evasive methods, such as altered and counterfeit passports and visas…[173]

As an example of the extent of the problem, in 2002, inspectors at land ports intercepted nearly 60,000 fraudulent documents.[174] GAO reported that one Southern Border port director advised them that about one-third of all port enforcement actions involved aliens falsely claiming United States citizenship. Another legacy INS official stated that false claims of U.S. citizenship were common.[175] False documents are a key to such attempts.

The task confronting the inspector of identifying fraudulent documents is daunting. Inspectors are forced to decide in a minute or less the validity of an overwhelming number of documents; as many as 200 countries use unique passports, official stamps, seals, and visas. More than 8,000 state and local offices issue different types of birth certificates, driver's licenses, and other documents that may be used fraudulently to gain entry into the United States. Inspectors stated that counterfeit IDs were readily available at the Mexican border, utilizing simple technology.

Many complained that when illegal immigrants were caught using fraudulent documents for attempted entry there were rarely any consequences. Local U.S. Attorney Offices' routinely decline to prosecute due to a lack of resources. The only consequence reported in most cases was the seizure of the fraudulent documents and denial of entry. One inspector stated it was the "equivalent of a thief who when caught stealing had no consequences for his actions." Inspectors at many of the larger ports-of-entry reported this has led to the proliferation of vendors openly "selling their wares" of fraudulent documents on the Mexican side of the border.

Better intelligence and training on document fraud was a common request of those interviewed on the border. An example of what can be accomplished with better training and intelligence is shown by the Pharr port-of-entry in McAllen, Texas. There, CBP has developed a world recognized database and program for fraudulent document detection. At this facility, al Qaeda training manuals and other terrorist writings on travel documents are used to extensively train inspectors from the United States as well as from foreign nations. One student, upon returning to his host country, credited this training in detecting the attempted entry of a terrorist with a "dirty bomb." As a result of this in-depth training, the Pharr seizure rate of fraudulent documents, averages as many as 400 a month, exceeding other ports-of-entry.

---

[173] *Op. Cit*., 9/11 Commission Report, p. 384.
[174] *Op. Cit*., GAO-03-782, p. 15.
[175] *Ibid*., p. 14-15.

Intelligence on Threat Level Increase Not Specific

In each city visited, the CBP Port Directors, Border Patrol Chiefs, agency managerial personnel and front line workers were questioned about the quantity and quality of specific information given to them when as the national threat level was increased. All responded that little, if any, useful information was given to assist them in evaluating the elevated threat at their specific location on the border. Managers at ports-of-entry reported they did not have clearances or secure faxes to receive specific intelligence concerning threat level increases and were generally dependent on notification from headquarters or other investigative agencies. Nevertheless, they did not receive any specific information they found useful for their important border mission.

The border managers stated when the threat level increased typically a general sense of heightened security was implemented with additional inspections and more referrals to secondary examinations.[176] Other consequences were additional overtime expenditures and significantly increased waiting periods for border crossing – for example, the waiting time increased by up to three hours in El Paso during the last code orange alert.

They also indicated that the increased threat level was an expensive proposition for the border agencies. CBP Congressional Affairs reported that the increase in security caused by the elevation to the orange level cost CBP, alone, more than $1.1 million a week and sustaining this level of operations for 30 days cost more than $80 million dollars.[177] Border community groups, including local Chambers of Commerce and mayors, across the border advised that the increased threat level added a significant fiscal burden on border trade, tourism, and security costs.[178]

A Proliferation of Intelligence Functions

One of the consequences of the need for more and better actionable intelligence has been the uncoordinated emergence of more intelligence functions. In March 2003, at the forming of DHS, the legacy Customs Service was divided into Customs and Border Protection (CBP) and the Immigration and Customs Enforcement (ICE). In the re-organization the intelligence function was transferred to ICE.

Interdiction agencies (CBP inspectors and Border Patrol agents) complained they were not receiving adequate intelligence on a timely basis to assist their responsibilities. They reported that although they provide ICE with intelligence gathered from interdictions, little information

[176] The staff found in Laredo, Texas, during orange alerts a 24/7 Port Director Command Center is activated, the number of Border Crossing Cards (BCC) entered into readers increased from 50% to 75%, all names of truck drivers are queried in TECS and the National Targeting Center (NTC) and the Laredo Document Analysis Unit (DAU) increase the number of inspections.

[177] Statistics provided to the Committee by CBP on August 17, 2004. Costs include personnel expenses associated with salaries and benefits and financial costs to include increased expenses for motor vehicles, aircraft fuel, etc., associated with more intensive inspections/monitoring at the border.

[178] Andy Soloman, The United States Conference of Mayors press release, *War, Threat Alert Increase City Security Costs by $70 Million per Week Nationwide*, March 27, 2003. Found at: http://www.usmayors.org/uscm/news/press_releases/documents/surveyrelease-032703.pdf.

was returned to allow CBP inspectors and Border Patrol agents to "close the loop or cycle" or "connect the dots" on smuggling patterns, trends, or most importantly, on suspected terrorist activity.

As a result, many CBP and Border Patrol offices have started developing "stand alone" intelligence units. This was especially noted in the many Border Patrol sectors. GAO has also identified the growth of these independent intelligence units, which often lack standard operating procedures and do not share information with other border agencies.[179]

General Patrick Hughes, DHS Assistant Secretary for Information Analysis acknowledged that there was limited sharing of databases/intelligence with federal agencies. He stated agencies have "shades of autonomy" which "are very much a concern." This, taken in consideration with the 9/11 Commission findings that "all" agencies are failing to share information, is an exploitable vulnerability on the border.

Partially contributing to this disjointed effort is that Border Patrol is still operating under pre-merger Memoranda of Understanding (MOU) to coordinate narcotic efforts with Drug Enforcement Agency, money laundering efforts with Internal Revenue Service, and national security issues with the Federal Bureau of Investigation. There is often no coordination with ICE, Border Patrol's investigative arm under DHS. As a result of these MOUs, the Border Patrol does not share the massive amounts of intelligence it develops through the capture of approximately one million illegal aliens a year with other border components of the Department of Homeland Security. Rather, following pre-merger policies, the Border Patrol shares this information with IRS, DEA and the FBI.[180]

An exception to this otherwise bleak intelligence picture was observed in the Arizona Border Control (ABC) initiative. This multi-agency initiative is driven with intelligence as its centerpiece. All agencies feed intelligence into a central command under the initiative called the "Intelligence Task Force and Reporting Center" (ITFRC). Once collected, this shared intelligence is then collated, analyzed, and disseminated back to the appropriate agencies as "actionable intelligence." This operation was uniformly viewed as effective and lauded as an example to be used elsewhere on the border to better coordinate the efforts of various border agencies.

---

[179] Despite the fact that federal land border agencies are responsible for more than 50% of the land on the Southern Border, a June 2004 GAO report found Border Patrol does not coordinate intelligence and threat assessments matters of concern with these agencies. See, U.S. Government Accountability Office, *Border Security: Agencies Need to Better Coordinate Their Strategies and Operations on Federal Lands,* GAO-04-590, (Washington, D.C., June 2004), p. 37.

[180] See, testimony of Robert C. Bonner, Commissioner, Customs and Border Protection, U.S. House, joint hearing of the Subcommittee on Infrastructure and Border Security of the Select Committee on Homeland Security and the Subcommittee on Criminal Justice, Drug Policy, and Human Resources of the Committee on Government Reform, *Counternarcotics at the Department of Homeland Security: How Well Are Anti-Drug Trafficking Operations Being Supported and Coordinated?,* July 22, 2004. Commissioner Bonner testified that "Border Patrol is one of the most robust collectors of human intelligence in law enforcement with more than one million apprehensions a year with thousands of intelligence reports a year."

Duplicative Intelligence Operations

Another concern raised is the number of intelligence and operations centers that may be duplicative and perhaps in competition with each other. Currently operating on the Southern Border are: the Border Patrol intelligence center, Operation Alliance; Border Patrol field intelligence units called BORFIC; Intelligence Collection Analysis Teams (ICAT) from ICE; High Intensity Drug Trafficking Area (HIDTA) multi-agency investigative intelligence groups; the High Intensity Financial Crime Area (HIFCAs); the Organized Crime Drug Enforcement Task Forces (OCDETF); the Joint Terrorism Task Force Six (JTF-6); and the El Paso Intelligence Center (EPIC). Joining these is the Border Interdiction Support Center (BOSIC) to be co-located at EPIC.[181] The latter was just announced in July by the DHS Counter Narcotic Officer, Roger Mackin who argued the need for one more intelligence center to combat the growing threat of illegal narcotics, widespread smuggling and potential terrorist activities on the Southern Border. It appears that this proliferation of intelligence and operations centers has led to stovepiping, the very thing DHS was formed to prevent.

Homeland Security Lacks Security Clearances to Investigate Terrorists

As noted, ICE is the primary investigative arm for DHS with a specific mission to prevent terrorism. Despite this mandate, the overwhelming majority of the ICE special agents on the Southern Border do not have Top Secret security clearances. In the majority of ICE offices visited, only two to three special agents assigned to the FBI Joint Terrorism Task Force (JTTF) and the head of the office had such clearances.[182] ICE management and agents alike complained that this situation interfered with investigations.

[181] Testimony of Roger Mackin, Director of Counter Narcotics, Department of Homeland Security, U.S. House, joint hearing of the Subcommittee on Infrastructure and Border Security of the Select Committee on Homeland Security and the Subcommittee on Criminal Justice, Drug Policy, and Human Resources of the Committee on Government Reform, *Counternarcotics at the Department of Homeland Security: How Well Are Anti-Drug Trafficking Operations Being Supported and Coordinated?,* July 22, 2004.

[182] ICE offices visited in Southern Border include Laredo, El Paso, Presidio, Tucson, Corpus Christi, Brownsville, McAllen, and San Diego.

Intelligence is a critical tool in the arsenal used by our border agencies to combat potential terrorists from crossing the border. Currently, intelligence is not being used effectively on the Southern Border. CBP inspectors, Border Patrol agents and ICE special agents, complained about the utility of the intelligence information currently received. It is neither enough nor timely. Unless it is improved, they cannot be expected to accurately and efficiently "connect the dots" and identify the terrorist threat on the Southern Border in a timely manner. Specifically, we recommend:

1. Consistent with the recommendations of the 9/11 Commission, the Administration must build an integrated, interoperable entry-exit system in a timely manner that links the databases of, and allows for, complete information sharing between each pillar of our border security and immigration control system: consular offices abroad, federal law enforcement, customs and border security agencies, and transportation agencies. As part of this system, it is imperative that the following occur:

- The IDENT/IAFIS integration process should proceed expeditiously as a national priority to avoid additional Resendez and Batres-type atrocities.
- Secondary inspection databases should be made interoperable immediately, thereby moving from the cumbersome eight-database system to a single consolidated system.
- This system should also interface with IBIS as an indicator to the first line officers for further examination of travelers.

2. There must be a coordinated federal approach for a uniform set of standards for all state driver's licenses and official identification cards to significantly reduce unauthorized persons from entering the United States by using fraudulent documents. In the interim, additional and re-occurring training for inspectors on detecting fraudulent documents should be required. Every port-of-entry should be provided a scanning system to interface with the DHS National Document Lab, whereby any questionable travel documents would be reviewed by highly trained document specialists for validity and authenticity. There must be certainty of consequences for violators apprehended with fraudulent documents.

3. When threat levels are raised, border officials must be provided greater guidance on the specific threat to the Southern Border and the additional security procedures that need to be implemented.

4. All ICE special agents and national security analytical support staff should receive Top Secret clearances. Newly trained ICE special agents should be processed for Top Secret clearances, similar to FBI and Secret Service special agents, at the completion of basic training.

Current ICE special agents in the field offices should have clearances up-graded during mandatory five-year background reviews.

5. Better coordination and cooperation is needed among border agencies to maximize intelligence driven operations and avoid duplicative intelligence functions. The Undersecretary for Border and Transportation Security should develop a strategy for intelligence collection, analysis and distribution; rationalize various collection and analytical units in the Directorate; and ensure that these units are fully coordinated with DHS' intelligence analysis officers.